THE UNITED STATES DISTRICT COURT FOR THE

DISTRICT OF UTAH

Northern Division

IN THE MATTER OF THE)

SEARCH OF:) **FILED UNDER SEAL**

[redacted])

[redacted]

to include outbuildings, sheds, and vehicles located on the property, and the persons of [redacted] and [redacted], should they be located on the property.

Case No. 2:21-mj-00166

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent Cody B. Tracy ("Your affiant") Homeland Security Investigations (HSI), being duly sworn under oath, do hereby depose and state, I am a Special Agent with HSI, assigned to the HSI Ogden, Utah office, being duly sworn, depose and state as follows to wit:

1. Your affiant has been so employed since September 2008. Your affiant is currently assigned as a Task Force Officer with the FBI Child Exploitation Task Force (CETF) which is run by the Salt Lake City FBI office. Prior to being employed by HSI, your affiant was employed as a Criminal Investigator/ Special Agent with the United States Secret Service for approximately six (6) years. As part of your affiant's duties as an HSI Special Agent, your affiant is charged to investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and

possession of child pornography in violation of Title 18 U.S.C. § 2252, 2252A, and 2251. Your affiant has received training in the area of child pornography and child exploitation.

2. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

FACTS AND CIRCUMSTANCES

3. The statements in this affidavit are based in part on information provided by law enforcement officers assigned to other law enforcement agencies, other special agents and employees of HSI and on your affiant's experience and background as a special agent of HSI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact known concerning this investigation. Your affiant has set forth only the facts are believed to be necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography); 18 U.S.C. § 2252(a)(4) (Possession of Child Pornography); 18 U.S.C. § 2252A(a)(1) (Transportation of Child Pornography) are located at:

- [redacted] to include outbuildings, sheds, and vehicles located on the property.
- **On the person of** [redacted] should he not be located at the [redacted] residence.
- **On the person of** [redacted] should she not be located at the [redacted] residence.

- **Green Ford Explorer,** [redacted], registered to [redacted] and [redacted].
- **Gray Dodge Ram 2500,** [redacted] registered to [redacted].
- **White Nissan Titan,** [redacted] registered to [redacted] and [redacted].
- **Person of** [redacted], **DOB** [redacted]
- **Person of** [redacted], **DOB** [redacted]

The property to be search is further described in Attachment A. The items to be searched and seized within this residence are further described in Attachment B of this affidavit. Your affiant is seeking authorization to search the above which are also described in Attachment B of this affidavit, attached hereto, for the items specified in Attachment B, attached hereto, which items constitute instrumentalities, fruits, and evidence of the foregoing violations. I am requesting authority to seize and search all items listed in Attachment B as instrumentalities, fruits, and evidence of crimes.

4. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. 2251(d) and (e) (advertising child pornography); 18 U.S.C. § 2252(a)(1) and (b)(1) (transportation of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(4)(B) and (b)(2)

(possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2251(d) and (e) prohibit any person from knowingly making, printing, or publishing, or causing to be made, printed, or published, or attempting or conspiring to make, print, or publish, or attempting or conspiring to cause to be made, printed, or published, any notice or advertisement seeking or offering to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or participating in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct; if such person knows or has reason to know that such notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed; or if such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed.

b. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual

depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

e. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

f. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs

typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality;

(c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

MOBILE DEVICES AND APPLICATIONS AND THE SEXUAL EXPLOITATION OF CHILDREN

7. Mobile devices such as mobile telephones, smart phones, cellular telephones, and tablets have become an increasingly popular medium used to facilitate the sexual exploitation of children. Mobile devices are relatively small in size (when compared to a laptop or a computer tower). Mobile devices also offer an increasing storage capacity for data, to include pictures and videos. Mobile devices also allow a user to access the Internet through either a data plan, or through free wireless, from anywhere. Mobile devices also allow a user to download any one of several applications which can be used to communicate with others via text, voice, or video. It is also relatively easy for a user to encrypt data on a mobile device or destroy data on a mobile device. A mobile device can also be used to transfer files from one device to another. This can be done by physically connecting a mobile device to a computer and transferring files, removing a

mobile device's internal storage (i.e. a micro SD card) and placing it in another device, transferring files wirelessly via a phone's Bluetooth capability, uploading files from the mobile device to a cloud storage account such as Dropbox, Google Drive, or Microsoft OneDrive, or using a mobile device as a wireless hotspot and allowing other devices (such as a laptop) to connect to the Internet. Your affiant also knows that individuals typically keep a mobile device in an area that they control, typically on their person, in their vehicle, or in their residence.

8. I know from training and experience that many involved in the sexual exploitation of children use mobile applications to facilitate the sexual exploitation of children. There are millions of applications or "apps" available for download to any user with access to the Internet. Popular apps, including Instagram, Facebook, Facebook Messenger, Whatsapp, Snapchat, and others, are commonly downloaded to a mobile device or smart phone (Although apps can also be downloaded to other internet connected devices like a desktop computer or laptop computer).

9. Many of these apps have a social media function which allows a user to create their own profile and communicate with other users. Depending on the application, the communication can occur as text messaging, voice messaging, and/or live stream video messaging. Apps also often allow for the sharing of files between users. These files can be images or videos and are often sent as attachments to a message. These files can then be stored online (for example in the message history or thread on an Internet Service Provider's servers) or downloaded to the individual's device.

10. Individuals with a sexual interest in children can and often do use social media applications to communicate with other individuals with a sexual interest in children. I have worked several cases where individuals with a sexual interest in children have used social media applications to obtain, distribute, and manufacture child pornography. I also know that

individuals with a sexual interest in children can, and often do use social media applications to communicate with minors for the purpose of obtaining sexually explicit images of the children with whom they are communicating. These individuals often use multiple applications to communicate with the victims and often create a profile where they pretend to be someone else. I have been involved in several investigations where an individual with a sexual interest in children has used social media mobile applications to communicate with children for the purpose of obtaining sexually explicit images and videos of the child, or for the purpose of meeting the child in person to engage in illegal sexual conduct.

BACKGROUND ON KIK

11. KIK advertises itself as "the first smartphone messenger with a built-in browser." KIK Messenger allows its users to "talk to your friends and browse and share any web site with your friends on KIK." KIK believes it is at the forefront of the "new era of the mobile web." KIK was founded in 2009 by a group of University of Waterloo students who started a company designed to "shift the center of computing from the PC to the phone." According to the website, KIK Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, KIK usernames - not phone numbers - are the basis for KIK user accounts, so KIK users are in complete control with whom they communicate. In addition, KIK features include more than instant messaging. KIK users can exchange images, videos, sketches, stickers and even more with mobile web pages.

12. The KIK app is available for download via the App Store for most iOS devices such as iPhones and iPads. Additionally, the KIK app is available on the Google PlayStore for

Android devices. KIK can be used on multiple mobile devices, to include cellular phones and tablets.

13. In general, providers like KIK ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address.

14. Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

15. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems or complaints from other users. Providers typically retain records about such communications, including records of e-mails and other contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

16. As explained below, information stored at MediaLab, parent company of KIK, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to

establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to an account that is retained by a provider like KIK can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up and other communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a KIK account at a relevant time. Further, such stored electronic data can show how and when the account was accessed or used. Such "timeline" information allows investigators to understand the chronological context of the usage of an account, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the user of a KIK account. Additionally, stored electronic data may provide relevant insight into the state of mind of the user of a phone number as it relates to the offense under investigation. For example, information relating to a particular KIK account may indicate the user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

17. KIK offers users the ability to create an identity within the app referred to as a "username". This username is unique to the account and cannot be changed. No one else can utilize the same username. A KIK user would have to create a new account in order to obtain a different username. The username for a particular KIK account holder is displayed in their KIK profile.

18. In October 2019, KIK was purchased by MediaLab, a company operating in the United States.

PROBABLE CAUSE

19. During February of 2021, your affiant reviewed one (1) CyberTipline Report submitted by Kik to the National Center for Missing and Exploited Children on November 11, 2020. Reference NCMEC CyberTipline Report [redacted]. This NCMEC report included six (6) videos of suspected child sex abuse material which was reviewed by your affiant. According to the report, NCMEC staff did not view any of the submitted materials and the files listed in the report are designated by "Hash Match." The "Hash Match" designation indicates that the uploaded files match the hash values of files previously viewed and categorized by NCMEC at the time the report was generated. Your affiant reviewed only the files submitted in the CyberTipline report and verified that the videos contain child pornography as defined by Federal Law.

20. Your affiant has reviewed NCMEC CyberTipline Report [redacted] dated November 11, 2021. A review of this report showed that on multiple dates in October 2020, a Kik user, who provided the name of [redacted] a username of [redacted] and an email address of [redacted] used Kik to upload/share six (6) videos containing child sex abuse material 15 times over a time period beginning on 10/19/2020 to 10/28/2020. It should be noted that according to this NCMEC report, all uploads of child sex abuse material originated from IP address [redacted] Additionally, this report listed the device used to register this account as a [redacted]

21. On or about February 10, 2021, your affiant reviewed the six (6) videos provided with NCMEC CyberTipline Report [redacted]. Below is a description of three (3) of the videos:

File Name: [redacted]

Upload Date/Time: 10-25-2020 00:43:59 UTC and 10-28-2020 20:37:04 UTC

Video Length: approximately 1 minute 44 seconds

Description: This video is approximately 1:44 in length. This video depicts what appears to be a prepubescent female wearing a gray pajama top and pink underwear dancing in front of a camera. A television with a cartoon playing is visible in the background along with a makeshift clothesline for hanging laundry. The child begins dancing and faces away from the camera, removes her underwear, and bends over, exposing her anus and vagina to the camera. The child then turns around, exposing her vagina to the camera and continues dancing in this manner. At another point, the child lifts up her pajama top and exposes her chest to the camera. Towards the end of the video, the child puts her underwear back on and turns off the camera. The child's face is clearly visible in portions of the video. The child appears to be between the ages of 6-8 years old.

File Name: [redacted]

Upload Date/Time: 10-28-2020 20:45:38 UTC, 10-19-2020 20:04:49 UTC, and 10-19-2020 20:04:56 UTC

Video Length: approximately 1 minute 56 seconds

Description: This video is approximately 1:56 in length. This video depicts what appears to be a nude prepubescent female lying on a bed with the camera focused on her genitalia. At this point an erect, adult male’s penis is visible being inserted into the child's

anus. The child is anally raped throughout the majority of the video. At one point, the adult male masturbates and appears to ejaculate all over the child's belly and crotch area. The camera then zooms in and focuses on the child's anus and vagina. At one point the child's face and chest is visible. After this, the video cuts to a different segment and it appears the child is being anally raped again until the video ends. The child appears to be between 6-8 years old.

File Name: [redacted]

Upload Date/Time: 10-28-2020 21:13:07 UTC

Video Length: approximately 1 minute 1 seconds

Description: This video depicts what appears to be a nude prepubescent female sitting on the lap of an adult female wearing a pink top and blue shorts. The adult female's face is visible throughout the entirety of the video. The child is sitting on the adult's lap with her legs spread, facing away from her. The child's vagina and chest are exposed to the camera. The adult female is rubbing the child's vagina with her right hand while the child uses both her hands to keep her legs spread open. The adult female continually rubs the child's vagina throughout the majority of the video. At one point the child goes over and appears to adjust the camera, then returns to the adult's lap where again the adult female rubs her vagina until the video ends. The child appears to be between the ages of 8-10 years old.

22. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address [redacted], which was used to upload the child sex abuse material to the Kik platform, is registered to Comcast.

23. On January 27, 2021, an HSI administrative summons (Summons number ICE-HSI-OU-2021-00019) was issued to Comcast for the assigned subscriber to IP address [redacted] on the dates and times for six (6) of the uploads of child pornography from the Kik user account with a username of [redacted] and an email address of [redacted] Your affiant also included the date of November 10, 2020, 09:15:41 UTC, as this date was reported on this CyberTipline report as a recent login for the user [redacted]

24. On February 1, 2021, your affiant received information from Comcast regarding summons ICE-HSI-OU-2021-00019 requesting subscriber records relating to the upload dates and times in question. According to the information received relating to upload referenced in the Kik report, the customer assigned this IP address for the relevant dates and times is as follows:

Subscriber Name: [redacted]

Service Address: [redacted]

Telephone #: [redacted]

25. On or about this same date, a CLEAR database search revealed that the address [redacted] **is** listed as the most recent place of residence for [redacted] according to public record. This search also revealed a [redacted] as being associated with this address. An NCIC criminal history check revealed no criminal history for either individuals. No other individuals were found to be associated with this address according to public record.

26. On February 3, 2021, your affiant observed a green Ford Explorer [redacted] parked in the driveway of the residence located at [redacted] Further investigation with the Utah DMV revealed this vehicle is registered to a [redacted] and [redacted]

27. On this same date, your affiant also observed a gray Dodge 2500 truck [redacted] parked in the driveway of the residence located at [redacted] Further investigation with the Utah DMV revealed the gray Dodge is registered to a [redacted]

28. On or about February 4, 2021, an HSI administrative summons (Summons number ICE-HSI-OU-2021-00021) was issued to Microsoft for user account information and IP logs for the user [redacted] which was registered to the Kik user who uploaded the CSAM according to the NCMEC CyberTipline report.

29. On February 11, 2021, a representative of the U.S. Postal Service stated that a [redacted] and a [redacted] are currently receiving mail at [redacted]. No further information regarding any other mail recipients was available at this time.

30. On February 16, 2021, your affiant observed a white Nissan Titan [redacted] parked in the driveway of the residence located at [redacted] Further investigation with HSI Sector Dispatch revealed the white Nissan is registered to a [redacted] and [redacted]

31. On February 18, 2021, Microsoft responded to HSI administrative summons ICE-HSI-OU-2021-00021. According to this response, the email [redacted] was registered to-

First Name: [redacted]

Last Name: [redacted]

Region/State: Utah

Postal Code: [redacted]

Creation Date (UTC): 9/21/1999 9:09:24 PM

According to Microsoft, the user had not logged into this account since March of 2020. It should be noted that according to these IP logs, the user of this email address had logged in from IP address [redacted] on December 5, 2019 and on February 13, 2020. This is the same IP address the user [redacted] had used to upload the CSAM to the Kik application in October of 2020 according to the NCMEC CyberTipline report. No HSI administrative summons was sent to Comcast for IP address subscriber information for the dates referenced above, as ISP's typically do not store this information for that amount of time based your affiant's past experience.

32. Your affiant is aware that the investigation in this case indicated that the activity in this case occurred via a mobile device. Because of this, data relevant to the investigation may be stored on digital media that may be found in many locations, including vehicles, or even pockets of clothing. Accordingly, your affiant requests this warrant authorize search of the defendant's vehicles and person, should they be located outside of the [redacted] **residence**.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

33. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or

camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

34. In the electronic world, it is possible to use pictures, images, and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey and idea, such as the use of a colon and parentheses ":)" to convey a smile or agreement) to discuss matters. Actual review of the contents of a photo-sharing account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

35. Collectors and distributors of child pornography often use online resources to retrieve, share, and store child pornography. Non-pornographic, seemingly innocuous images of minors are often found in accounts that also contain child pornography, or that is used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images. Further, the online services

allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. The online storage accounts are often free but can involve a charge. A subscriber assigned a free online storage account frequently can set up such accounts by providing limited identifying information. Any information provided is frequently fictitious in an attempt to preserve the anonymity of the user. Consequently, even if it is known that a collector or distributor of child pornography is a subscriber of a free online storage service, the service provider frequently will have no records in that subscriber's name. Instead, the online service will only be able to identify files, including child pornography, that are associated with a "login," or unique, user-created identity the subscriber uses to "log on" to the online service. Such an online storage account is particularly useful to a collector or distributor of child pornography. Such a subscriber can collect, store, view and distribute electronic images, including child pornography, directly from the online service. Consequently, the illegal files have minimal contact with the subscriber's home computer. The subscriber can also manipulate the files on an online storage service from any computer connected to the Internet. Nonetheless, evidence of an online storage account is often found on a home computer of a user subscribing to such a service. Evidence of an online storage account may take the form of passwords located in encrypted, archived, or other files on the user's home computer. Other evidence can also be found through unique software that may exist on a user's home computer that has been developed by the online storage service. This unique software will frequently contain evidence not only of the existence of such accounts, but the login and password.

36. I know from training and experience that a person trading in, receiving, transporting, distributing, or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation.

37. I know from training and experience that digital evidence is not limited to computers. I have been involved in cases where persons engaged in the type of crime under investigation can access the Internet, display images reflecting their interests or participation in the crime and communicate with other individuals with the same interests using digital storage devices to include cellular telephones, email devices, and personal digital assistants. These devices are frequently found to contain chat communications in the form of short message service (SMS) messages as well as enabling Internet and digital cellular network access.

38. I know from training and experience that the complete contents of online accounts may be important to establishing the actual user who has dominion and control of an online account at a given time. Online accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. So, information stored in connection with an online account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation. This helps establish and prove each element of the crime or alternatively, may exclude the innocent from further suspicion. In my training and experience, an online user's account activity, IP log, location information, search history, stored electronic communications, and other data retained by providers, can indicate who has used or controlled an online account

or can provide context for the crime under investigation. This can include evidence of motive and intent to commit a crime (e.g., communications about planning crimes), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. Further, account activity, especially when paired with other evidence of the crime, can show how and when the account was accessed or used, and may reflect a user's motive or state of mind when doing so. For example, as described herein, providers log the Internet Protocol (IP) address from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Especially when considered in context with other evidence, such information allows investigators to understand the geographic and chronological contest of an account's access, use, and events relating to the crime under investigation. Location data also helps with this. Providers allow users to "tag" their location in posts to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the account user or other suspects.

39. I know from training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or code words (which require entire strings or series of email conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as

a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey and idea, such as the use of a colon and parentheses ":)" to convey a smile or agreement) to discuss matters. Keyword searches would not account for any of these possibilities, so actual review of the contents of an online account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

40. I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in **Attachment B** in order to prevent unnecessary invasion of privacy and overbroad searches. I have learned through practical experience that various emails often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between communication threads and contents of accounts, and any respective attachments, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. Therefore, to obtain the full picture and meaning of the data from the information sought in **Attachment B** of this application, and to maintain its admissibility at trial, the Government needs to maintain access to all the resultant data. The completeness and potential of probative value of the data must be

assessed within the full scope of the investigation. As with all evidence, the Government will obtain the contents of the items in its custody and control, without alteration.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

41. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, advertise, transport, distribute, receive, possess, and/or access with intent to view child pornography, including:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines,

negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

f. Such individuals also may correspond with and/or meet others to share

---

1 *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if an individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices)..

16. Based on the following, I believe that the user of Kik username [redacted] residing at the SUBJECT PREMISES likely displays characteristics common to individuals who produce, advertise, transport, distribute, receive, possess, and/or access with intent to view child pornography. This opinion is based on your affiant's opinion that [redacted] is linked to the sharing of child pornography, and the associated IP address used to upload the suspected child pornography resolved to the residence as described above. As detailed herein, the target of the investigation distributed suspected child pornography via Kik. In order to distribute such materials, the user would necessarily have to acquire and possess child pornography.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

42. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

(A) Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

(B) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the

file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

(C) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

(D) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

44. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat

programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the

records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

45. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives,

flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

46. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an

individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

47. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. It is intended this warrant will allow for repeated forensic review up to and including the time of trial

BIOMETRIC ACCESS TO DEVICES

48. As part of Report 1 Kik provided information indicating that the Kik account in question was registered using a model of cellular device listed as and uses an operating system known as Android. This model number is associated with the Samsung Galaxy S-20 mobile device model. Your affiant conducted research and learned that Samsung Galaxy S-20 possibly uses various biometric options to access and/or secure this model device. It is your affiant's opinion that the device used to create this Kik account likely enjoys Biometric security. This warrant

permits law enforcement to compel all individuals present at the subject premises including but not limited to [redacted] and [redacted] to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-

facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that

would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of [redacted] and [redacted], to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of [redacted]

and [redacted] and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face [redacted] and [redacted] activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that [redacted] and [redacted] state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to ask [redacted] and [redacted] to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

50. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

51. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the property listed in Attachment A and the seizure of items listed in Attachment B.

Request for Sealing

52. It is respectfully requested this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, affidavit and search warrant. Your affiant believes that sealing this document is necessary because the target of this investigation may have the ability to remotely destroy evidence of these offenses, should he become aware of the extent of this investigation. Disclosure of these materials would give the target of the investigation an opportunity to destroy evidence, change patterns of behavior, notify

confederates or possibly flee from prosecution.

CODY B TRACY Digitally signed by CODY B TRACY Date: 2021.03.05 10:18:13 -07'00'

Cody Tracy

Special Agent

Homeland Security Investigations

Sworn and subscribed before me this 9th day of March 2021.

HON DUSTIN B. PEAD

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

Person of [redacted] dob [redacted]

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § § 2251(d), 2252 and 2252A and are contained in the items:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
    a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, [redacted] including utility and telephone bills, mail envelopes, or addressed correspondence;
    b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
    c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
    d. Records and information relating to the sexual exploitation of children, including correspondence and communications between Kik users;
    e. Records and information showing access to and/or use of Kik; and
    f. Records and information relating or pertaining to the identity of the person or persons using or associated with Kik Username [redacted]

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel all individuals present at the subject premises to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the DEVICES found at the PREMISES, and

(b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that [redacted] and [redacted] state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

1. As described above and in Attachment B, this warrant allows law enforcement to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

2. If a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by

an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

3. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In

my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein

may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. When an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. A computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

4. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. During the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search.

In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition,

computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

5. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

6. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. It is intended this warrant will allow for repeated forensic review up to and including the time of trial